IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Wallman	**Conf. No.**:	1382
Serial No.:	10/667,852	**Art Unit**:	2439
Filed:	9/22/2003	**Examiner**:	Tolentino, R.
Title:	**SYSTEM AND METHOD FOR PROVIDING PHYSICAL WEB SECURITY USING IP ADDRESSES**	**Docket No.**:	CHA920030022US1 (IBMC-0076)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This is an appeal from the Final Rejection dated May 24, 2010, rejecting claims 1, 4-5, 7-9, 11, 14-15 and 17-22. As Appellant has paid the requisite fee set forth in 37 C.F.R. 41.20(b)(2) for the previously-filed Appeal Brief of November 20, 2008, and that Appeal Brief was not officially considered, this appeal is not accompanied with that fee.

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case included claims 1-16. Claims 17-22 were added during prosecution. Claims 1, 4-5, 7-9, 11, 14-15 and 17-22 remain pending, stand rejected, and form the basis of this appeal. Claims 2-3, 6, 10, 12 and 16 have been cancelled.

STATUS OF AMENDMENTS

A Response, filed on March 9, 2010 in response to the Non-Final Action dated December 9, 2009, did not result in the allowance of the claims.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides a system for providing security for an internet server (independent claim 1), a method for authenticating a user accessing an Internet server (independent claim 7) and a program product stored on a recordable medium for providing security for an Internet server (independent claim 11).

The system for providing security for an Internet server (independent claim 1) includes: a logical security system (e.g., Logical Security System 14, FIG. 1; page 4, line 11) for processing login and password data (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) received from a client device (e.g., CLIENT DEVICE 24, FIG. 1; page 4, line 23-page 5, line 1) during a server session with the Internet server (e.g., SERVER 10, FIG. 1; page 4, line 16) in order to authenticate a logged in user (e.g., USER 20, FIG. 1; page 4, line 16); a physical security system (e.g., Physical Security System 16, FIG. 1; page 4, lines 11-12) for processing Internet protocol (IP) address information (e.g., IP Address 26, FIG. 1; page 5, line 5) of the client device at the Internet server in order to authenticate the client device for the duration of the server session; and

a memory system (e.g., Memory System 13, FIG. 1; page 4, line 14) for storing, at the Internet server, a list of each logged in user and a reference IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) collected during a login procedure, wherein the logical security system is configured to access the list to authenticate the logged in user, and wherein the physical security system is configured to separately access the list in order to authenticate the client device; wherein the physical security system includes a proxy server module (e.g., Proxy Server Module 36, FIG. 2; page 6, line 20) for comparing only an incomplete portion of an IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) obtained from a received message (Messages 29, FIG. 1, page 5, line 16) against only a like incomplete portion of the reference IP address for the logged in user.

The method for authenticating a user accessing an Internet server (independent claim 7) includes: storing in a memory system (e.g., Memory System 13, FIG. 1; page 4, line 14), at the Internet server (e.g., SERVER 10, FIG. 1; page 4, line 16), a reference Internet protocol (IP) address (e.g., IP Address 26, FIG. 1; page 5, line 5) and associated login data (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) whenever a new server session is initiated on the Internet server from a client device (e.g., CLIENT DEVICE 24, FIG. 1; page 4, line 23-page 5, line 1); receiving a message (e.g., Messages 29, FIG. 1; page 5, line 16) from a requesting user (e.g., USER 20, FIG. 1; page 4, line 16) at the Internet server; obtaining login data (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) accompanying the message; obtaining an IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) from a message header in the message; determining if the login data of the requesting user is currently listed in the memory system as an existing session with the Internet server; and if the login data of the requesting user is currently listed, determining at the Internet server if the IP address from the received message matches the reference IP address associated with the login data of the requesting user, the determining of the

IP address including examining only an incomplete portion of the IP address of the requesting user and determining if the incomplete portion matches only a like incomplete portion of the reference IP address.

The program product for providing security for an Internet server (independent claim 11) includes: a component for (e.g., Logical Security System 14, FIG. 1; page 4, line 11) processing logical security information (e.g., Initial Security Info 28, FIG. 1; page 5, line 1) received from a client device (e.g., CLIENT DEVICE 24, FIG. 1; page 4, line 23-page 5, line 1) during a server (e.g., SERVER 10, FIG. 1; page 4, line 16) session in order to authenticate a logged in user (e.g., USER 20, FIG. 1; page 4, line 16); a component for (e.g., Physical Security System 16, FIG. 1; page 4, lines 11-12) processing Internet protocol (IP) address information (e.g., IP Address 26, FIG. 1; page 5, line 5) of the client device in order to authenticate the client device during the server session by comparing the IP address of a received message (e.g., Messages 29, FIG. 1; page 5, line 16) against the list of IP addresses stored by the server; and a component for storing, at the Internet server, a list of each logged in user and a respective reference IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) collected during a login procedure, wherein the component for processing logical security information is configured to access the list to authenticate the logged in user, and wherein the component for processing IP address information is configured to separately access the list to authenticate the client device; wherein the component for processing IP address information includes a proxy server module (e.g., Proxy Server Module 36, FIG. 2; page 6, line 20) for comparing only an incomplete portion of an IP address (e.g., IP Address 26, FIG. 1; page 5, line 5) obtained from a received message (Messages 29, FIG. 1, page 5, line 16) against only a like incomplete portion of the reference IP address for the logged in user.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) Whether claims 1, 4, 7-9, 11, 14 and 17-22 are unpatentable under 35 U.S.C. 103(a) over Ramachandran et al. (US 2003/0084343, "Ramachandran") in view of in view of Hay (US 2002/0120868) and Barnes (US 7,382,787).

(2) Whether claims 5 and 15 are unpatentable under 35 U.S.C. 103(a) over Ramachandran in view of Hay, and in further view of Muratov et al. (U.S. PG-Pub. No. 2003/0097596, "Muratov").

ARGUMENT

(1) Rejection of claims 1, 4, 7-9, 11, 14 and 17-22 over Ramachandran, Hay and Barnes under 35 U.S.C. 103(a).

The rejection under 35 U.S.C. 103(a) is defective because the references Ramachandran, Hay and Barnes, taken alone or in combination, fail to disclose or suggest each and every feature of the claims.

With respect to the rejections, Appellant respectfully reiterates the arguments made in the Amendments of 4 September 2009 and 9 March 2010. Appellant has amended the claims in those respective Amendments solely to further prosecution of this application, which has been pending since 22 September 2003, and received a first Office Action on 9 May 2007, over three (3) full years ago. Appellant further notes that a Pre-Appeal Brief Conference Request (11 January 2008) and a separate Appeal Brief (20 November 2008) have been filed during prosecution, and in both cases, prosecution has been re-opened. In view of this protracted prosecution history, Appellant thanks the Board for considering the following arguments.

With respect to independent claim 1, the Examiner posits that the newly added reference (Barnes), when viewed along with Ramachandran and Hay, teaches or suggests, "... a proxy server module for comparing only an incomplete portion of an IP address obtained from a received message against only a like incomplete portion of the reference IP address for the logged in user..." (Claim 1)(emphasis added). Appellant respectfully submits that the Examiner is mistaken. Specifically, Barnes describes a process in which node IP addresses in a binary trie are compared to adjacent node IP addresses to determine routing and switching paths through the trie. (*See*, Barnes at col. 31, line 46-col. 32, line 66). This method of Barnes is performed in a progressive manner through the trie, such that each level of nodes on the tree farther from the

root will contain an additional bit (per node) as compared to the previous level of nodes. (*Id.*). Specifically, this method of Barnes includes progressively "checking" nodes farther out on the trie in order to determine if that node is a "leaf" node (last in its line). (*Id.* at col. 32, lines 14-16, and 53-57). For example, Barnes reads, "[a]ccordingly, only the 13th bit, i.e., the next most significant bit is checked for the next branch." (*Id.* at col. 32, lines 53-57). That is, Barnes teaches "checking" the last bit to determine whether that bit is a "0" or a "1". (*Id.* at col. 32, lines 57-60). At best, Barnes' method could be considered comparing a portion of an IP address against a reference table including either a "0" or a "1." Barnes does not, however, teach "…comparing only an incomplete portion of an IP address obtained from a received message against only a like incomplete portion of the reference IP address for the logged in user…" (Claim 1). That is, Barnes does not teach comparing only incomplete portions of two distinct IP addresses against one another. (*See*, claim 1)(paraphrasing for explanatory purposes).

Additionally, Barnes is silent regarding, "…comparing only an incomplete portion of an IP address obtained from a received message against only a like incomplete portion of the reference IP address for the logged in user…" (Claim 1)(emphasis added). As discussed herein, Barnes is aimed at a "Packet Routing and Switching Device." (Barnes at Title). Barnes does not teach or suggest that the IP address it is "checking" could be "obtained from a received message" or a "reference IP address for [a] logged in user." (*Contrast* Barnes *with* Appellant's claim 1). Further, nothing in Barnes even remotely suggests that its teachings would be useful in a "system for providing security for an Internet server." (See, claim 1). That is, Barnes does not use its method of "checking" for anything other than finding routing and switching paths in a binary trie. (See generally, Barnes). Barnes fails to suggest that its teachings could be applied to a security-related system as in Appellant's claim 1.

The Examiner alleges the following regarding combining Barnes, Hay and Ramachandran, "...it would have been obvious to a person of ordinary skill in the art to use Barnes' Packet routing and switching with Ramachandran's one protocol web access to usage data in a data structure of a usage based licensing server because it offers the advantage of reducing the risk that Packets are dropped." (Final Office Action of May 24, 2010 at 4). The Examiner fails, however, to indicate why a person of ordinary skill in the art would have used the teachings of either of Ramachandran or Barnes (or, for that matter, Hay) to apply Barnes' routing and switching methods. Nothing in any of the references suggests that checking a single, final bit of an IP address for a "0" or a "1" (e.g., as in Barnes) would be beneficial in a security-related application. As such, Appellant respectfully submits that the Examiner has failed to meet his burden of making a prima facie case of obviousness.

Accordingly, Appellant respectfully submits that independent claim is not rendered obvious by the combination of Ramachandran, Hay and Barnes.

Appellant submits that the other independent claims (claim 7 and claim 11) not specifically addressed herein include features similar to at least those described with reference to claim 1, above. Accordingly, Appellant respectfully submits that claims 7 and 11 are similarly not rendered obvious by the combination of Ramachandran, Hay and Barnes.

Appellant also notes that the Examiner's interpretation of dependent claim 17 (as well as dependent claims 18 and19) in the above-referenced Final Office Action is incorrect. (Final Office Action at page 8, item no. 11). Specifically, the Examiner alleges that Hay teaches, "...wherein the incomplete portion of the IP address includes the first characters of the IP address..." (Claim 17). Specifically, the Examiner continues to allege, as he has in previous Office Actions (e.g., December 9, 2009) that the term "portion" means an entire IP address.

(Final Office Action at page 8, item no. 11). While Appellant has already addressed this issue in a previous response, Appellants note that the Examiner has neglected a term in the claim in making his current outstanding rejection. That is, the claim reads in part, "...the incomplete portion of the IP address..." (Claim 1)(emphasis added). Therefore, the portion of the IP address referred to in this claim is by definition "incomplete." It is not, in any way, the "entire address" as posited by the Examiner. (Office Action at page 8, item no. 11). As such, Appellant respectfully submits that the rejections of claims 17-19 are deficient.

(2) Rejection of claims 5 and 15 is over Ramachandran, Hay and Muratov under 35 U.S.C. 103(a).

The rejection under 35 U.S.C. 103(a) is defective because the references Ramachandran, Hay and Muratov, taken alone or in combination, fail to disclose or suggest each and every feature of the claims.

Regarding dependent claims 5 and 15, Appellant hereby incorporates the arguments made with respect to independent claim 1, from which claim 5 depends. Muratov fails to overcome the deficiencies Ramachandran and Hay, addressed above. (See Item No. 1).

Accordingly, Appellant submits that all pending claims are allowable because Ramachandran, Hay, Barnes and/or Muratov, taken alone or in combination, fail to teach or suggest each and every feature of the claims as required by 35 U.S.C. 103(a).

Respectfully submitted,

/Matthew B. Pinckney/

Matthew B. Pinckney
Reg. No. 62,727

Date: 20 September 2010

Hoffman Warnick, LLC
75 State Street, 14th Floor
Albany, New York 12207
Phone: (518) 449-0044
Fax: (518) 449-0047

CLAIMS APPENDIX

1. A system for providing security for an Internet server, comprising:

a logical security system for processing login and password data received from a client device during a server session with the Internet server in order to authenticate a logged in user;

a physical security system for processing Internet protocol (IP) address information of the client device at the Internet server in order to authenticate the client device for the duration of the server session; and

a memory system for storing, at the Internet server, a list of each logged in user and a reference IP address collected during a login procedure, wherein the logical security system is configured to access the list to authenticate the logged in user, and wherein the physical security system is configured to separately access the list in order to authenticate the client device;

wherein the physical security system includes a proxy server module for comparing only an incomplete portion of an IP address obtained from a received message against only a like incomplete portion of the reference IP address for the logged in user.

4. The system of claim 1, wherein the physical security system terminates the session for the user if the incomplete portion of the IP address obtained from the received message does not match the like incomplete portion of the reference IP address for the logged in user.

5. The system of claim 4, wherein the physical security system deletes all instances of the logged in user from the stored list if the incomplete portion of the IP address obtained from the received message does not match the like incomplete portion of the reference IP address for the logged in user.

7. A method of authenticating a user accessing an Internet server, comprising:

storing in a memory system, at the Internet server, a reference Internet protocol (IP) address and associated login data whenever a new server session is initiated on the Internet server from a client device;

receiving a message from a requesting user at the Internet server;

obtaining login data accompanying the message;

obtaining an IP address from a message header in the message;

determining if the login data of the requesting user is currently listed in the memory system as an existing session with the Internet server; and

if the login data of the requesting user is currently listed, determining at the Internet server if the IP address from the received message matches the reference IP address associated with the login data of the requesting user, the determining of the IP address including examining only an incomplete portion of the IP address of the requesting user and determining if the incomplete portion matches only a like incomplete portion of the reference IP address.

8. The method of claim 7, comprising the further step of initiating a login procedure if the login data of the requesting user is not currently listed in the memory system.

9. The method of claim 7, comprising the further step of terminating all server sessions listed in the memory system having the login data of the requesting user if the incomplete portion of the IP address from the obtained message does not match the like incomplete portion of the reference IP address.

11. A program product stored on a recordable medium for providing security for an Internet server, the program product comprising:

a component for processing logical security information received from a client device during a server session in order to authenticate a logged in user;

a component for processing Internet protocol (IP) address information of the client device in order to authenticate the client device during the server session by comparing the IP address of a received message against the list of IP addresses stored by the server; and

a component for storing, at the Internet server, a list of each logged in user and a respective reference IP address collected during a login procedure, wherein the component for processing logical security information is configured to access the list to authenticate the logged in user, and wherein the component for processing IP address information is configured to separately access the list to authenticate the client device;

wherein the component for processing IP address information includes a proxy server module for comparing only an incomplete portion of an IP address obtained from a received message against only a like incomplete portion of the reference IP address for the logged in user.

14. The program product of claim 11, wherein the component for processing IP address information terminates the session for the user if the incomplete portion of the IP address obtained from the received message does not match the like incomplete portion of the reference IP address for the logged in user stored in the list.

15. The program product of claim 14, wherein the component for processing IP address information deletes all instances of the logged in user from the stored list if the incomplete portion of the IP address obtained from the received message does not match the like incomplete portion of the respective reference IP address for the logged in user.

17. The system of claim 1, wherein the incomplete portion of the IP address includes the first characters of the IP address.

18. The method of claim 7, wherein the incomplete portion of the IP address includes the first characters of the IP address.

19. The program product of claim 11, wherein the incomplete portion of the IP address includes the first characters of the IP address.

20. The system of claim 1, wherein the IP address information is received from a proxy server capable of sending a plurality of IP addresses assigned to a plurality of client devices, and wherein the IP address includes the incomplete portion which is constant for each of the plurality of IP addresses.

21. The method of claim 7, wherein the IP address information is received from a proxy server capable of sending a plurality of IP addresses assigned to a plurality of client devices, and wherein the IP address includes the incomplete portion which is constant for each of the plurality of IP addresses.

22. The program product of claim 11, wherein the IP address information is received from a proxy server capable of sending a plurality of IP addresses assigned to a plurality of client devices, and wherein the IP address includes the incomplete portion which is constant for each of the plurality of IP addresses.

EVIDENCE APPENDIX

No evidence has been submitted.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.